

# MA357 — Elementary Number Theory

Spring, 2012

Fernando Q. Gouvêa

People have always been fascinated by numbers and their properties. Number theory is the natural outgrowth of that fascination. One finds questions about “properties of numbers” already in ancient mathematics. Since then, number theory has become an important part of the western mathematical tradition. Because it deals with patterns that are easily observed empirically, it sometimes has the feel of experimental science. On the other hand, the proofs that these patterns hold (or that they don’t) are often hidden so deeply that one needs extremely sophisticated mathematical tools to make any progress at all. It is perhaps this blend of simplicity (in the questions) and depth (in the answers) that has led mathematicians such as Gauss to proclaim number theory “the Queen of Mathematics.”

During most of its history, number theory was famous for being the purest of “pure mathematics.” Even as late as 1982, when Jean Dieudonné wrote his *Panorama of Pure Mathematics* (check it out, it’s in the library), he could claim that there were no contacts between number theory and the physical sciences. That has all changed, quite suddenly, over the last few decades, when two new realms of application became more and more important. The first is computer science, where number theory has come to play a crucial role in the problems of encoding data and of encrypting data. The second is theoretical physics, where recent developments in string theory and related ideas have led to surprising connections with number theory.

Of course, it never was quite true that number theory had no applications: in any situation that is discrete, one is bound to run into number-theoretical problems, and one can mention several examples beginning in the mid-nineteenth century. The difference, I think, is that those examples involved application of relatively elementary number theory, while modern-day applications have grown increasingly subtle and have in fact motivated new work in the field. This course will pay some attention to the appli-

cations of number theory, especially those related to cryptography, but our main focus will be on the theory itself. Nevertheless, I will try to give you pointers to significant applications as we reach the relevant portions of the course.

So what is number theory about? It is about (whole) numbers, but in a special sense. Number theory isn't really too interested in specific problems about particular numbers (that's arithmetic); instead, it focuses on *general* patterns. Some theorems of number theory are known by everyone: the sum of two odd numbers is odd, for example. Some are harder. We will prove, for example, that a prime number can be written as a sum of two squares if and only if it leaves a remainder of 1 when it is divided by 4. We will discuss a number of questions of this type in our first class meeting.

This course will be an introduction to elementary number theory. The word "elementary" here has a technical meaning: it indicates that we won't be using more advanced theories (such as complex analysis or algebraic geometry) to study number-theoretical patterns. This means the course has few pre-requisites, but it does *not* mean that the material is easy — in fact, many of the theorems we'll be thinking about are quite subtle.

One way to approach elementary number theory is to keep away from "heavy" mathematical concepts from, say, abstract algebra or analysis. To do this, one chooses simple but tricky methods to prove the basic theorems. Unfortunately, this suggests that number theory is all about finding incredibly tricky elementary arguments. That's just not true! So we're going to try something different, choosing arguments and ideas that link to bigger mathematical themes. So, for example, when it comes time to prove something known as "Fermat's Little Theorem," we will introduce the concept of a commutative group. The proof will then follow from a general theorem about groups. This way, I hope you will see how number theory fits into the rest of mathematics. Perhaps it'll also help convince you that those other ideas are useful!

I think number theory is fun. I hope you'll come to agree.

**Goals of this Course:** What do I expect you to be able to do after this course? Of course, I want you to know the content. But here are some other goals:

- I hope you will further develop your ability to read, understand, and create mathematical arguments.

- I hope you will leave the course more confident in your ability to think creatively and to find solutions to problems without having a “road map” in advance.
- I hope you will improve your ability to think precisely.
- I hope you will improve your ability to *write* about mathematics.
- I hope you will realize that things can be fascinating despite being difficult (maybe even *because* they are difficult).
- I hope you will have a better sense of this area of mathematics: know its central themes, be able to use some of its basic methods, be able to enjoy new ideas and discoveries.
- Finally, I hope you will have a stronger desire to learn more mathematics!

**Office hours:** I will be in my office and available for questions, discussion, and general conversation at the following times:

Tuesdays, 1:00–3:00 PM

Wednesdays and Fridays, 1:00–2:00 PM

If you can't come during any of these times, please call and make an appointment.

Please do not hesitate to come see me — in fact, I strongly encourage you to come. It is part of your education, and one of your privileges as a Colby student.

**Where to find me:** Here's the basic information:

office: Mudd 412

phone: 5836

email: fggouvea

If you need to reach me when I'm not in my office, email is the best method. I'm usually pretty quick at answering email.

**Texts:** Our textbook will be *Elements of Number Theory*, by John Stillwell. This is not an easy book, but its approach matches well with what I want to achieve in this course. We will probably work through chapters 1–7 and 9.

We have a second required book, John Derbyshire’s *Prime Obsession*. This is not a textbook; rather, it’s a “popular math” book. I hope you’ll find it readable. Our approach to Number Theory will emphasize what is often described as the “algebraic” side of number theory. Derbyshire’s book will give us a glimpse of another branch of advanced number theory, known as “analytic number theory.”

**Other books:** It’s important to remember that Colby does have a good library. We have many books on number theory, and it’s quite possible that one of them will fit your personal style and so prove to be a useful complement to Stillwell. The number theory books live in the sections of the library numbered QA241–247. Some books I like are the ones by Davenport, Hardy and Wright, Niven and Zuckerman, Sierpinski, Baker, Cohen (a two-volume monster) and Hua Loo Keng. There is also *The Book of Numbers*, by Conway and Guy, that presents itself very informally but is really quite serious. Joe Silverman has a book called *A Friendly Introduction to Number Theory*; if you find Stillwell hard to read, Silverman might help.

A different set of books would be relevant to those of you who like to use computers to investigate mathematics. Pride of place goes to two books:

- *A Course in Computational Number Theory* by Bressoud and Wagon, which uses *Mathematica* to explore the properties of numbers, and
- *Elementary Number Theory: Primes, Congruences, and Secrets*, by Stein, which uses SAGE. Colby’s library has this as an e-book, so you can access it easily.

Also interesting are the books by Bach and Shallit, Crandall and Pomerance, and Riesel.

The number theory I’m most interested in has an *algebraic* flavor (in the sense of abstract algebra). One of the best starting places to learn more about that is *A Classical Introduction to Modern Number Theory*, by Ireland and Rosen. See also the books by Murty, Neukirch, Stewart–Tall, and, if you like an historical approach, Edwards.

It might be fun to look at books that highlight the applications of Number Theory. For example, *Number Theory in Science and Communication*,

by M. R. Schroeder, *The Unreasonable Effectiveness of Number Theory*, ed. by S. Burr, *From Number Theory to Physics*, ed. by M. Waldschmidt et. al., and pretty much any book on cryptography.

In other words, whatever your interests, don't limit yourself to the required books. Go explore. Read the introductions. Read a few chapters. Skip over uninteresting details. Have fun. If you like, ask me for further suggestions of things to read.

**Technology:** Number theory has an experimental side: one can detect number patterns by computing a large number of examples. You will probably find it useful to use either a calculator or a computer to construct examples, test conjectures, and experiment. For the first part of the course, a calculator may be sufficient (but if your calculator doesn't do infinite-precision arithmetic you should watch out for rounding errors). To deal with bigger numbers, however, one absolutely needs to use a computer program that can do integer arithmetic. If you're familiar with *Mathematica*, you're welcome to use that. What I really recommend, however, is a very powerful suite of mathematical software tools called SAGE. It is free, and you can either download it to your computer from [sagemath.org](http://sagemath.org) or use it online (after creating a free account) at [sagenb.org](http://sagenb.org). For those who like older stuff, there is also GP, which has been incorporated into SAGE but can still be downloaded and run on its own: go to [pari.math.u-bordeaux.fr](http://pari.math.u-bordeaux.fr).

**Assignments:** There will be a variety of assignments during the course:

- **Automathography by email:** your first assignment is to send me a short email message introducing your mathematical self to me. Tell me about courses you have taken, about ideas that you've found exciting, about things you've found boring or difficult, about your goals as a student. If you have taken MA274, I'd like to know what that was like and how much you remember. If you have worries about any special problems or needs, let me know. You are encouraged to be creative in your response; don't just answer the questions above, but include whatever else you wish. This email message is due no later than **Wednesday, February 8**.
- **First writing assignment: review a book.** There will be two writing assignments. The first will be based on John Derbyshire's *Prime Obsession*. You will be asked to read the book and then write a review.

Your review should describe the content of the book, discuss the quality of the expository writing, and give your reaction to both the mathematics and the history that Derbyshire explains. More details about this assignment will be provided during the first week of classes. This assignment will be due **Friday, March 9**.

- **Second writing assignment: a mathematical exploration.** The second writing assignment will involve some expository mathematical writing of your own. I will provide you with a list of possible topics, all of which will consist either of a significant theorem or a problem (solved or unsolved) that requires some exploration. (It's ok for you to choose your own topic, of course, but check with me first.) This paper has a dual goal: to understand a small bit of mathematics as thoroughly as possible, and then to explain it as clearly as possible. More details of this assignment will be provided later. This assignment will be due **Friday, April 27**.
- **Problem Sets:** Problem sets will be passed out every **Monday beginning on February 6** and will be **due the following Monday**. These will include a few routine practice problems and a few more interesting problems that will require some thought and creativity. These problem sets *will* take several days to complete: don't leave them for the last day! See the handout *On Writing Up* for information on what is expected and on how these assignments will be graded.

**Exams:** We will have one midterm exam, in the second week of March (the week before spring break), and also a final exam. Both exams will be take-home exams. I will provide more information as we get nearer to the exam dates.

**Grading:** Your grade will be computed as follows:

problem sets	20%
writing assignments	30%
midterm exam	20%
final exam	30%

**Attendance:** You are expected to come to class. Should you be unable to come to class on a particular day, please contact me. Unexcused absences *will* have an effect on your grade for the course. As per college rules, many unexcused absences may lead to your being asked to withdraw from the course.

**Cheating and Plagiarism:** You are encouraged to interact with others as you do your assignments (in fact, it will be a lot more fun doing it that way). The written work that you turn in, however, must be your own. You may, of course, seek help from any and all sources, but in the end what you write must be a result of your own thought processes and your grappling with the material. Feel free to discuss any questions you have about this with me. Also, please read the Colby policy on academic honesty as stated in the College Catalogue.

**On reading your textbook:** I expect you to read your textbook. This doesn't mean that you have to learn everything by yourself, but it does mean that I will often concentrate on the central ideas of an argument when the book contains all the details. Of course, you should feel free to ask questions about what's in the book when we discuss the material in class.

Reading a mathematics book is not like reading other texts. First of all, it's slow. Mathematicians tend to write in a very compressed, terse style, and reading it takes lots of "unpacking." As you read, have paper and pencil in hand, and be careful to work out examples, fill in details, check assertions. Second, one reading is not going to be enough. I suggest that before each class you try to read the relevant sections of the book. In this first reading, you should try to get the overall structure of the argument, without worrying too much about the details. Then, after class, re-read the section, comparing with what we discussed in class and filling in all the details you can. If necessary, compare with other books. Discuss the material with other people, and with me. Then read again.

**Working with others:** Mathematics is a social activity. Mathematicians are always talking to each other, explaining questions and theorems and saying things like "what's really going on here is... ", "do you know whether... " and "I have a conjecture... " You'll enjoy this course more if you can find a small group of people to work with, not only doing the homework together, but talking about the material. The more you invest, the more you'll profit.

**Web site :** Our course web site is at

<http://www.colby.edu/personal/fqgouvea/357>

Go there. I'll try to post all the course handouts and other interesting stuff.

**A tentative schedule:** Here is the tentative schedule, with a list of readings for each week. This is very ambitious, and I won't hesitate to change it as we go along, but I hope it will give you some idea of what we will be covering and of what to read in preparation for each class.

**Feb. 1–3** Introduction, induction, division with remainder (1.1–1.3).

**Feb. 6–10** Binary, simple diophantine equations (1.4–1.8)

**Feb. 13–17** GCD and unique factorization, linear diophantine equations (2.1–2.8)

**Feb. 20–24** Integers mod  $n$ , groups, Fermat's Little Theorem (3.1–3.5)

**Feb. 27–Mar. 2** Inverses mod  $k$ , quadratic diophantine equations, primitive roots (3.6–3.9)

**Mar. 5–9** RSA cryptography, Pell's equation (4.1–5.3).

**Mar. 12–16** More on Pell's equation, quadratic forms (5.4–5.8). Midterm.

**Mar. 19–23** Spring Break.

**Mar. 26–Mar. 30** Gaussian integers (6.1–6.7)

**Apr. 2–6** Quadratic integers (7.1–7.4).

**Apr. 9–13** More on quadratic integers (7.5–7.7).

**Apr. 16–20** Quadratic reciprocity (9.1–9.8)

**Apr. 23–27** Failure of unique factorization; ideals.

**May 1–4** Number theory in  $\mathbb{Z}[\sqrt{-5}]$ .